DS-KD9203-FE6

Video Intercom Face Recognition Door Station with 4.3-inch Screen

User Manual

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED “AS IS” AND “WITH ALL FAULTS AND ERRORS”. HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN

CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Note	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction

Warning

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Caution

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.

- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

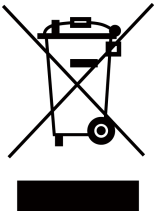
1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

Industry Canada ICES-003 Compliance
This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:
(1) this device may not cause interference, and
(2) this device must accept any interference, including interference that may cause undesired operation of the device.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Contents

1 Appearance

Door Station without Fingerprint Module

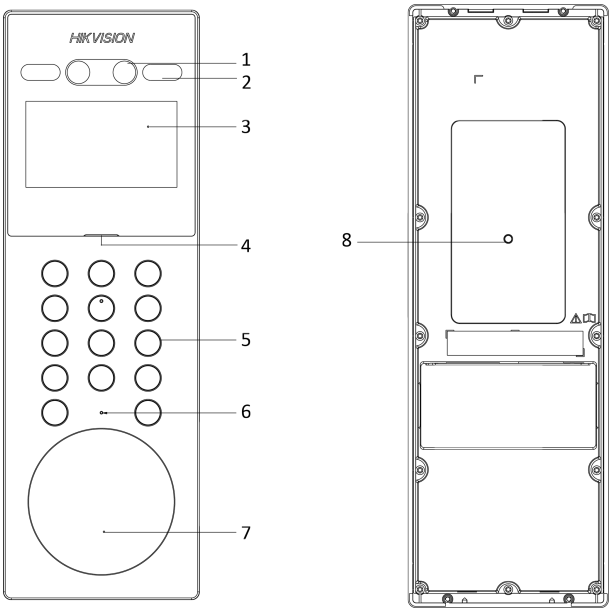


Figure 1-1 Appearance of Door Station without Fingerprint Module

Table 1-1 Description

No.	Description
1	Camera
2	IR Supplement Light
3	Screen
4	Loudspeaker
5	Buttons

No.	Description
6	Microphone
7	Card Reading Area
8	TAMPER

Door Station with Fingerprint Module

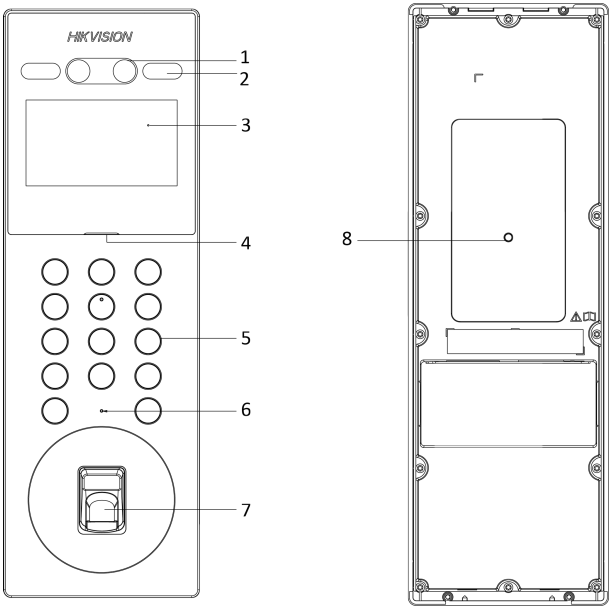


Figure 1-2 Appearance of Door Station with Fingerprint Module

Table 1-2 Description

No.	Description
1	Camera
2	IR Supplement Light
3	Screen

No.	Description
4	Loudspeaker
5	Buttons
6	Microphone
7	Card Reading Area/ Fingerprint Recognition Module
8	TAMPER

2 Terminal and Wiring Description

2.1 Terminal Description

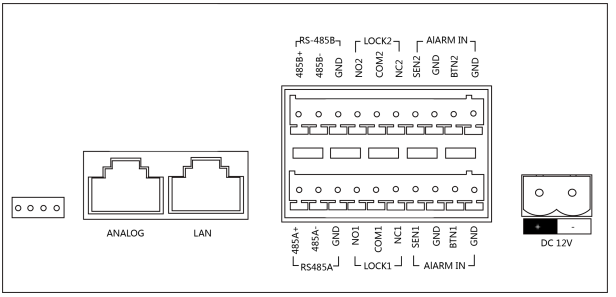


Figure 2-1 Terminal Description

Table 2-1 Description

Name	Terminal	Description
Network Interface	ANALOG	Analog Signal Input
	LAN	Network Signal Input
ALARM IN	SEN1	Door Contact Input 1
	SEN2	Door Contact Input 2
	BTN1	Exit Button Input 1
	BTN2	Exit Button Input 2
	GND	Grounding
RS-485	485A+	External RS-485 Card Reader
	485A-	
	485B+	External Elevator Controller
	485B-	

Name	Terminal	Description
DOOR	NC1	Door Lock Relay Output 1(Normally Close)
	COM1	Common Interface 1
	NO1	Door Lock Relay Output 1(Normally Open)
	GND	Grounding
	NC2	Door Lock Relay Output 2(Normally Close)
	COM2	Common Interface 2
	NO2	Door Lock Relay Output 2(Normally Open)
	GND	Grounding
Power Supply	DC 12 V	12 VDC Power Input

Note

- Alarm input interface cannot be edited. Refers to the actual model.
- You can only wire the SEN1/SEN2 terminal with the door contact. And wire the BTN1/BTN2 terminal with the exit button.

2.2 Wiring Description

2.2.1 Door Lock Wiring

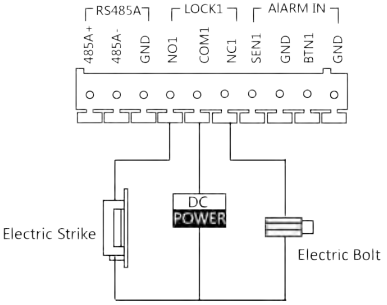


Figure 2-2 Door Lock Wiring

Note

- Terminal NC1/COM1 is set as default for accessing electric bolt. Terminal NO1/COM1 is set as default for accessing electric strike.
- To connect electric lock in terminal NO2/COM2/NC2, it is required to set the output of terminal NO2/COM2/NC2 to be electric lock with **iVMS-4200** Client Software.

2.2.2 Exit Button Wiring

Wire the BTN1/BTN2 terminal with the door contact.

Here takes BTN1 for example.

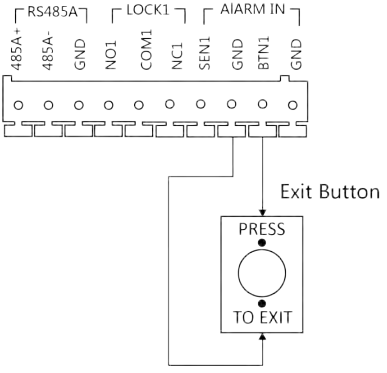


Figure 2-3 Exit Button Wiring

2.2.3 Alarm Input Device Wiring

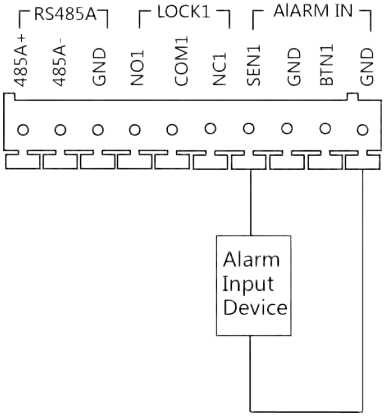


Figure 2-4 Alarm Input Device Wiring

2.2.4 Door Contact Wiring

Wire the SEN1/SEN2 terminal with door contact.

Here takes SEN1 for example.

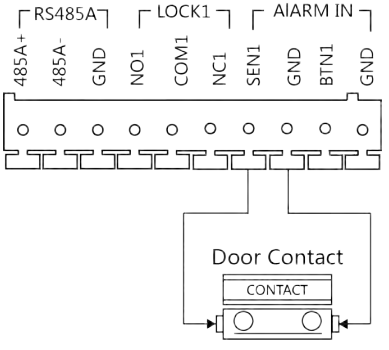


Figure 2-5 Door Contact Wiring

3 Installation

Note

- Make sure the device in the package is in good condition and all the assembly parts are included.
- The power supply the door station supports is 12 VDC. Please make sure your power supply matches your door station.
- Make sure all the related equipment is power-off during the installation.
- Check the product specification for the installation environment.

3.1 Gang Box

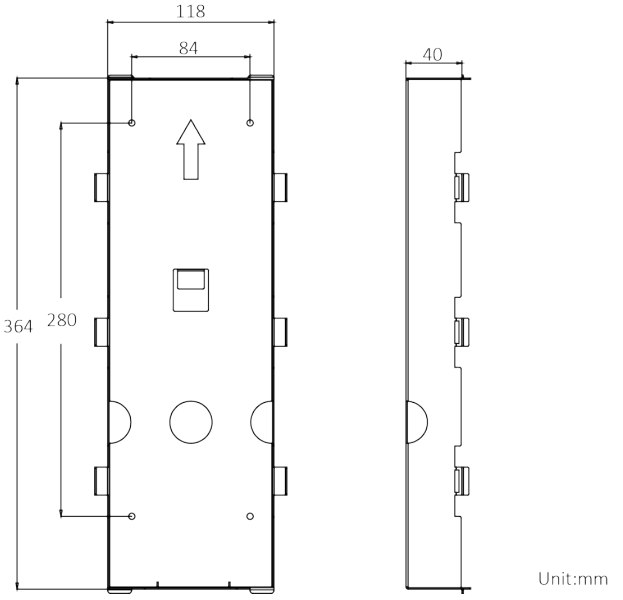


Figure 3-1 Dimension of the Gang Box

Note

- The dimension of the gang box is 364 mm (W) × 118 mm (H) × 40 mm (D).
- The installation hole should be bigger than the actual size. The suggested dimension of the installation hole is 364.3 mm (W) × 118.6 mm (H) × 40.2 mm (D).

3.2 Flush Mounting with Gang Box

Steps

1. Cave an installation hole in the wall. Pull the cable out from the wall.

   Note

   - The suggested dimension of the installation hole is 364.3 mm (W) × 118.6 mm (H) × 40.2 mm (D).
   - The suggested length of the cables left outside is 250 mm.

2. Install the gang box into the wall.
   1) Remove the plastic sheet of the gang box with the tool.
   2) Insert the gang box into the installation hole. Mark the gang box screw holes' position with a marker, and take out the gang box.
   3) Drill 4 holes according to the marks on the wall, and insert the expansion sleeves into the screw holes.
   4) Fix the gang box with 4 expansion bolts.
3. Fix the gap between the gang box and wall with concrete. Remove the mounting ears with tool after concrete is dry. Connect the cables according to the *Wiring Description*.
4. Insert the door station into the gang box. Slide the door station down and fix it with 2 set screws. Apply Silicone sealant among the joints between the device and the wall (except the lower side) to keep the raindrop from entering.

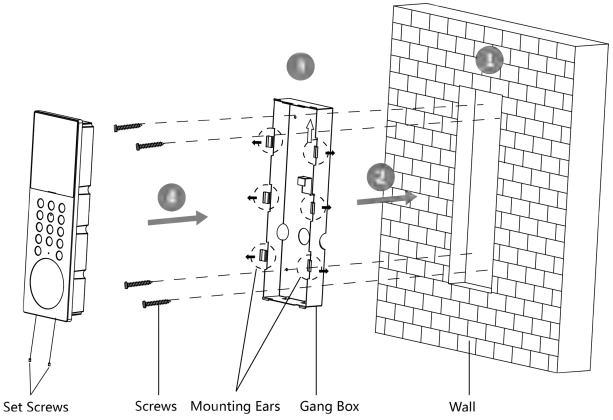


Figure 3-2 Flush Mounting with Gang Box

4 Activation

4.1 Activate Device Locally

You are required to activate the device first by settings a strong password for it before you can use the device.

Steps

1. Power on the device to enter the activation page automatically.
2. Create a password and confirm it.
3. Tap **OK** to activate the door station.

4.2 Activate Device via Client Software

You can only configure and operate the door station after creating a password for the device activation.

Default parameters of door station are as follows:

- Default IP Address: 192.0.0.65.
- Default Port No.: 8000.
- Default User Name: admin.

Steps

1. Run the client software, click **Maintenance and Management → Device Management → Device** to enter the page.
2. Click **Online Device**.
3. Select an inactivated device and click **Activate**.
4. Create a password, and confirm the password.

Note

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

5. Click **OK** to activate the device.

Note

- When the device is not activated, the basic operation and remote operation of device cannot be performed.
- You can hold the **Ctrl** or **Shift** key to select multiple devices in the online devices, and click the **Activate** button to activate devices in batch.

5 Local Operation

5.1 Video Intercom Operation

5.1.1 Call Resident

The door station can work as main/sub door station, and outer door station, which correspond to different calling resident modes respectively.

Call Resident from Main/Sub Door Station

Press call button to enter the calling page.

Enter the room No. and press call button.

Call Resident from Outer Door Station

Press call button to enter the calling page.

Enter【Building No. + # + Unit No. + # + Room No.】 and press call button to call resident.

5.1.2 Call Center

Press call button to enter the calling page.

Press center button to call. Press * to cancel during calling management center.

5.2 Unlock Door

5.2.1 Unlock by Password

Unlock by Common Password

Press call button to enter the calling page.

Enter 【# + Room No. + Common Password + #】 to unlock the door.

Note

The default common password is 123456.

Unlock by Public Password

Note

Make sure you have created the public password via iVMS-4200 Client Software remotely.

Press call button to enter the calling page.

Enter 【# + Public Password + #】 to unlock the door.

5.2.2 Unlock by Swiping Card

Note

Make sure you have issued the card to the device. Refers to *User Management* for details.

Present the card on the card reading area to unlock.

5.2.3 Unlock by Fingerprint

Note

Make sure you have added the fingerprint to the device. Refers to *User Management* for details.

Put your finger on the finger recognition module to unlock.

5.2.4 Unlock by Face

Note

Make sure you have added your face picture to the device. Refers to the *User Management* for details.

Face forward at the camera to unlock.

6 Configuration via Client Software

6.1 Edit Network Parameters

To operate and configure the device via LAN (Local Area Network), you need connect the device in the same subnet with your PC. You can edit network parameters via **iVMS-4200** client software.

Steps

1. Select an online activated device and click the **Modify Netinfo**.
2. Edit the device IP address and gateway address to the same subnet with your computer.
3. Enter the password and click **OK** to save the network parameters modification.

Note

- The default port No. is 8000.
- The default IP address of the door station is 192.0.0.65.
- After editing the network parameters of device, you should add the devices to the device list again.

6.2 Add Device

You should add device to the software so as to configure the device remotely.

6.2.1 Add Online Device

Before You Start
Make sure the device to be added is in the same subnet with your computer. Otherwise, please edit network parameters first.

Steps

1. Click **Online Device** to select an active online device.
2. Click **Add**.
3. Enter corresponding information, and click **Add**.

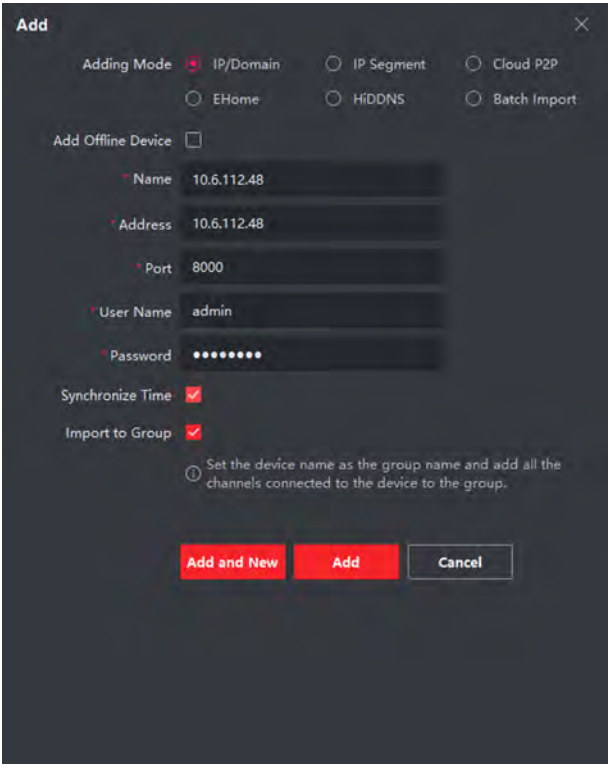


Figure 6-1 Add to the Client

6.2.2 Add Device by IP Address

Steps

1. Click **+Add** to pop up the adding devices dialog box.
2. Select **IP/Domain** as **Adding Mode**.
3. Enter corresponding information.
4. Click **Add**.

6.2.3 Add Device by IP Segment

You can add many devices at once whose IP addresses are among the IP segment.

Steps

1. Click **+Add** to pop up the dialog box.
2. Select **IP Segment** as **Adding Mode**.
3. Enter corresponding information, and click **Add**.

6.3 Remote Configuration

Select the device, click ⚙ to configure the parameters remotely.

6.3.1 System

Click **System** on the remote configuration page to display the device information: Device Information, General, Time, System Maintenance, User, and RS-485.

Device Information

Click Device Information to enter device basic information page. You can view basic information (the device type, and serial No.), and version information of the device.

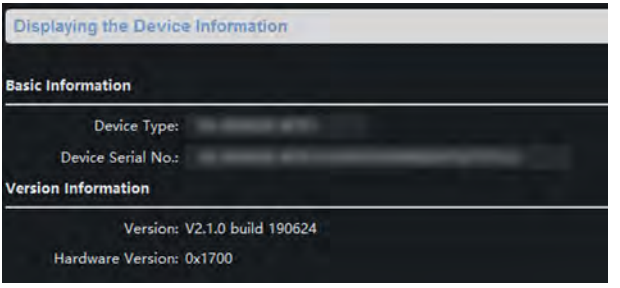


Figure 6-2 Device Information

General

Click **General** to enter device general parameters settings page. You can view and edit the device name and device ID.

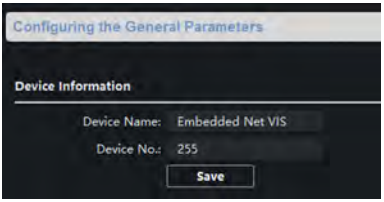


Figure 6-3 General

Time

Click **Time** to enter the device time settings page.

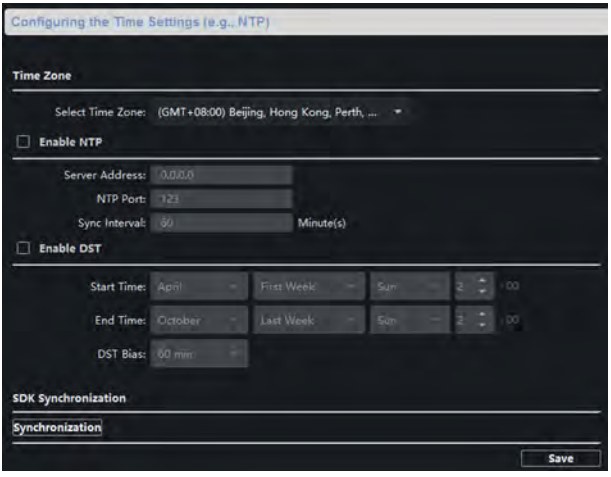


Figure 6-4 Synchronize Time

Select **Time Zone** or **Enable NTP**. Click **Save** to save the time settings.

- Time Zone
  - Select a time zone from the drop-down list menu.
  - Click **Synchronization**.
- NTP

- Check the checkbox of Enable NTP to enable NTP.
- Enter the server address, NTP port, and synchronization interval.

- DST
  - Check the checkbox of Enable DST to enable DST.
  - Enter the start time and end time of DST, and set the DST bias.

Note

The default port No. is 123.

System Maintenance

Click **System Maintenance** to enter the page.

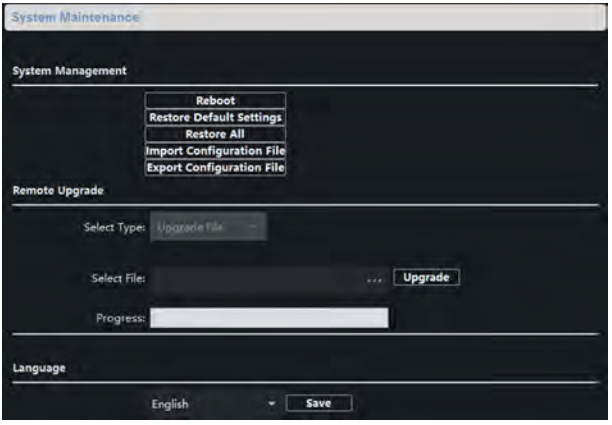


Figure 6-5 System Maintenance

- Click **Reboot** and the system reboot dialog box pops up. Click **Yes** to reboot the system.
- Click **Restore Default Settings** to restore the default parameters.
- Click **Restore All** to restore all parameters of device and reset the device to inactive status.

Note

- Click **Restore Default Settings**, all default settings, excluding network parameters, will be restored.
- Click **Restore All**, all default settings, including network parameters, will be restored. The device will be reset to inactivated status.

- Click **Import Configuration File** and the import file window pops up. Select the path of remote configuration files. Click **Open** to import the remote configuration file. The configuration file is imported and the device will reboot automatically.
- Click **Export Configuration File** and the export file window pops up. Select the saving path of remote configuration files and click **Save** to export the configuration file.
- Click **...** to select the upgrade file and click **Upgrade** to remote upgrade the device. The process of remote upgrade will be displayed in the process bar.
- Select a language, and click **Save** to change the device system language.

Note

- The device supports 11 languages: English, Russian, German, Italian, French, Portuguese, Spanish, Turkish, Arabic, Polish, and Vietnamese.
- Rebooting the device is required after you change the system language.

User

Click **User** to enter the user information editing page.

Select the user to edit and click **Modify** to enter the user parameter page.

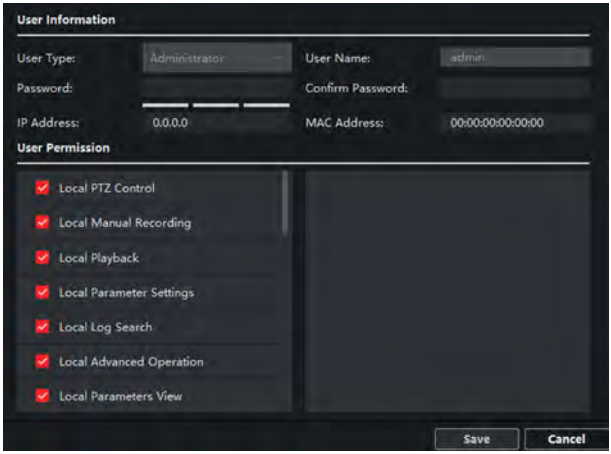


Figure 6-6 User Page

Note

- The new password and confirm password should be identical.
- After editing the password of device, click refresh button from the device list, the added device will not be there. You should add the device again with new password to operate the remote configuration.

RS-485

Click **RS485** to enter the RS-485 settings page. You can view and edit the RS-485 parameters of the device.

Figure 6-7 RS-485 Settings

Note

For indoor station and master station, there are 3 choices for the working mode: transparent channel, disable, and custom.

6.3.2 Video Intercom

Click **Video Intercom** to enter the Video Intercom Settings page.

Device ID Configuration

Steps

1. Click **ID Configuration** to enter the device ID configuration page.

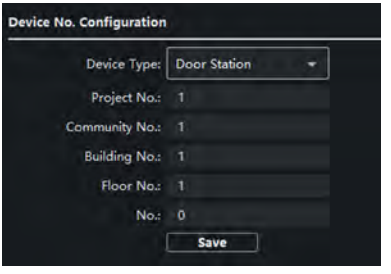


Figure 6-8 Device No. Configuration

2. Select the **device type** from the drop-down list, and set the corresponding information.

Note

The device type select **Door Station** as default. You can select **Outer Door Station** to change the device type.

3. Click **Save** to enable the device number configuration.

Note

- For main door station, the serial No. is 0.
- For sub door station, the serial No. is higher than 0. Serial No. ranges from 1 to 99.
- For each villa or building, at least one main door station should be configured, and sub door stations can be customized.
- For one main door station, at most 8 sub door stations can be customized.

Time Parameters

Steps

1. Click **Time Parameters** to enter time parameters settings page.

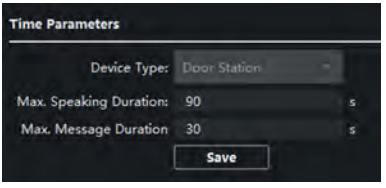


Figure 6-9 Time Parameters

2. Configure the maximum ring duration, maximum live view time, and call forwarding time.
3. Click **Save**.

Note

For door station, maximum speaking time and maximum message time should be configured. Maximum speaking time varies from 90 s to 120 s, and maximum message time varies from 30 s to 60 s.

Permission Password

Steps

1. Click **Permission Password** to enter the settings page.
2. Select **Type** of the password.
3. Edit the password.
4. Click **Save** to enable the settings.

Access Control and Elevator

Before You Start

- Make sure your door station is in the mode of main door station. Only the main door station support elevator control function.
- Connection between the door station and the elevator controller supports network interface.

Steps

1. Click **Access Control and Elevator** to enter corresponding configuration page.

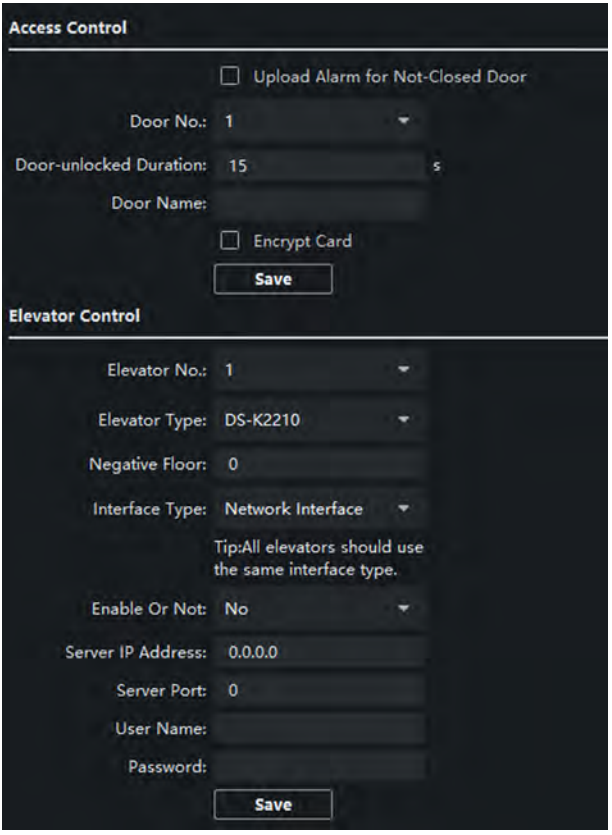


Figure 6-10 Access Control and Elevator

2. Set the **Access Control** parameters.

1) Select the door No.
2) Set the **Door-unlocked Duration**.
3) **Optional:** Enable **Upload Alarm for Not-Closed Door**.
4) Click **Save** to enable the settings.

Note

- The door-unlocked duration ranges from 1 s to 255 s.
- If you check **Upload Alarm for Not-Closed Door**, an alarm will be triggered automatically if the door is not locked in the configured duration.
- Enabling **Card Encrypt**, the door station can recognize the encrypted information of the card when you swiping the card on the door station.

3. Set the **Elevator Control** parameters.
   1) Select an elevator No., and select an elevator controller type for the elevator.
   2) Set the negative floor.
   3) Select **network interface** as **interface type**. Enter the elevator controller's IP address, port No., user name, and password.
   4) Enable the elevator control.

Note

- Up to 4 elevator controllers can be connected to one door station.
- Up to 10 negative floors can be added.
- Make sure the interface types of elevator controllers, which are connected to the same door station, are consistent.

I/O Input and Output

Steps

1. Click **I/O Input and Output** to enter the I/O input and output settings page.

Figure 6-11 I/O Input and Output

2. Select **I/O input No.**, **input mode**, **output No.**, and **output mode**.
3. Click **Save** to enable the settings.

Note

- For door station, there are 4 I/O input terminals. By default, Terminal 1 and 2 correspond to Door Status. Terminal 3 and 4 correspond to interfaces of Door Switch.
- For door station, there are 2 I/O Output Terminals. Terminal 1 and 2 correspond to Door interfaces (NO1/COM/NC1; NO2/COM/NC2) of door station. Door 1 is enabled by default. You can enable/disable IO Out according to needs.

Volume Input and Output

Steps

1. Click **Volume Input/Output** to enter the volume input and output page.
2. Slide the slider to adjust the **Volume Input** and **Volume Output**.
3. Click **Save** to enable the settings.

Face and Fingerprint Settings

Steps

1. Click **Face and Fingerprint** to enter the settings page.
2. Configure the parameters.
3. Click **Save** to enable the settings.

Advertisement Settings

Steps

1. Click **Advertisement** to enter the settings page.
2. Select the **Mode**.
3. Click **+** to add the picture.
4. Slide to set the duration.
5. Click **Save** to enable the settings.

Note

- Up to 5 pictures can be added. Picture formats requires JPG. The size of the pictures should be less than 1MB. The switching duration of the picture ranges from 1 to 10 seconds. Refers to the Appendix C for the details.
- When the device has no ads, the default picture displayed on the main page.

6.3.3 Network Settings

Click **Network** to enter the Network Settings page.

Local Network Configuration

Steps

1. Click **Local Network Configuration** to enter local network configuration page.

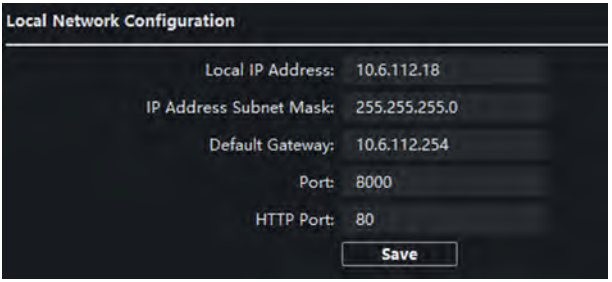


Figure 6-12 Local Network Configuration

2. Enter the **Local IP Address**, **Subnet Mask**, **Default Gateway**, **Port** and **HTTP Port**.
3. Click **Save** to enable the settings.

Note

- The default port No. is 8000.
- After editing the local network parameters of device, you should add the devices to the device list again.

Linked Device Network Configuration

Before You Start

On the linked devices network configuration page, you can configure the network parameters of master stations, SIP servers and management centers of the same LAN. The devices can be linked to the door station and realize the linkage between these devices.

Steps

1. Click **Linked Network Configuration** to enter linked network configuration page.

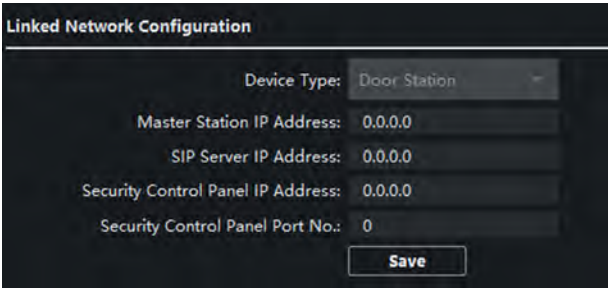


Figure 6-13 Linked Device Network

2. Enter the **Master Station IP Adderss**, **(Main) Door Station IP Address**, **SIP Server IP Address**, **Security Control Panel IP Address** and **Port No.**
3. Select the main door station type from the drop-down list.
4. Click **Save** to enbale the settings.

Note

- After adding master station IP Address, the linkage between indoor station and master station can be realized.
- After adding the door station IP Address, the video intercom between indoor stations of same building can be realized.
- After adding SIP Server Address IP, the video intercom of same community: video intercom between indoor stations of different building, calling indoor station from outer door station and video intercom between management center and indoors.
- After adding management center IP Address, the events can be uploaded to the management center.
- For indoor extension, only parameter about the main indoor station should be configured.

FTP

After configuring the FTP parameters, the captured pictures of door station will be uploaded to the FTP server automatically.

Steps

1. Click **FTP** to enter the FTP parameters settings page.

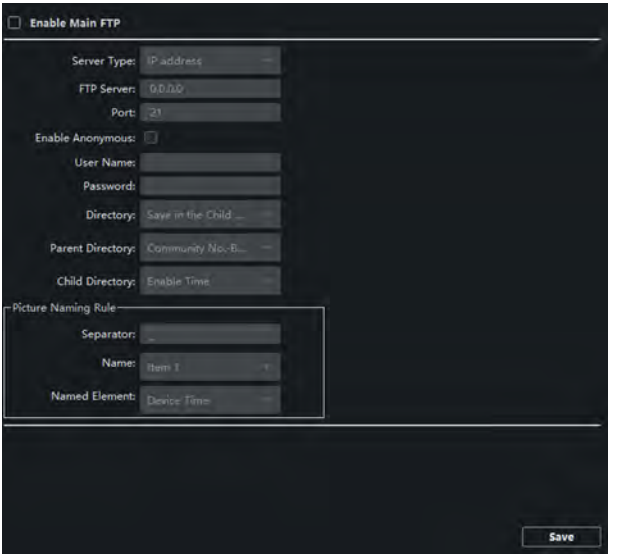


Figure 6-14 FTP Settings

2. Enable **Enable Main FTP**.
3. Select IP address from the drop-down list of server mode.
4. Enter the FTP server address, and port No.
5. **Optional:** Enable the anonymity.
6. Enter the name and password.
7. Select the directory structure and set the separator, naming item, and naming element.
8. Click **Save** to enable the settings.

Note

- The default port No. is 21.
- To enable anonymity or not is according to whether the FTP server enables anonymity.

Advanced Settings

Steps

1. Click **Advanced Settings** to enter the advanced network settings page.

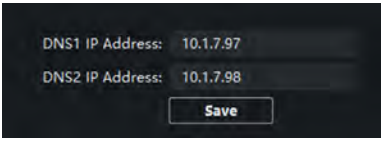


Figure 6-15 Advanced Settings

2. Enter the DNS server addresses.
3. Click **Save** to enable the settings.

6.3.4 Video Display Settings

Click **Video Display** to enter the Video Display Settings page.

Video Parameters

Steps

1. Click **Video Parameters** to enter the video parameters settings page.

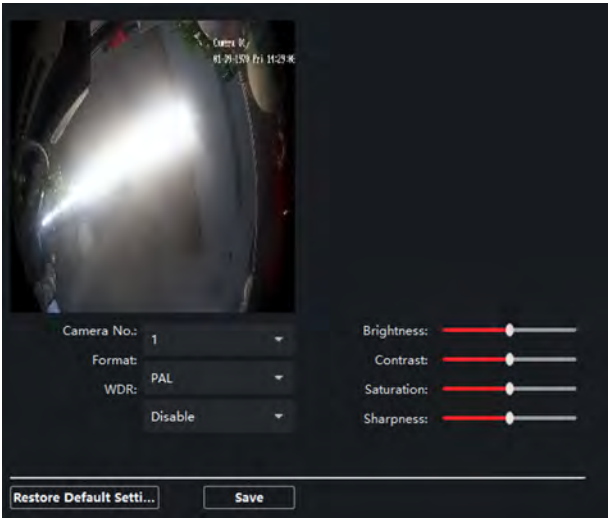


Figure 6-16 Video Parameters

2. Select the **Camera No.**
3. Select the video standard (PAL and NTSC can be selected).
4. **Optional:** Enable **WDR** mode.
5. Set the **Brightness**, **Contrast**, **Saturation** and **Sharpness** of the video.
6. Click **Save**.

Note

Click **Restore Default Settings** to restore all video parameters excluding network parameters to the factory settings.

Video & Audio

Steps

1. Click **Video & Audio** to enter the video parameters settings page.

Figure 6-17 Video & Audio

2. Set the parameters.
3. Click **Save**.

Note

It's suggested to keep the default settings to ensure the video/image quality.

6.4 Device Management

Device management includes device activation, adding device, editing device, and deleting device, and so on.

After running the iVMS-4200, video intercom devices should be added to the client software for remote configuration and management.

6.5 Organization Management

On the main page of the Client Software, click **PersonalManagement** to enter the configuration page.

6.5.1 Add Organization

Steps

1. In the organization list on the left, click **+Add**.
2. Enter the **Organization Name** as desired.
3. Click **OK** to save the adding.

4. **Optional:** You can add multiple levels of organizations according to the actual needs.
   1) You can add multiple levels of organizations according to the actual needs.
   2) Then the added organization will be the sub-organization of the upper-level organization.

   Note

   Up to 10 levels of organizations can be created.

6.5.2 Modify and Delete Organization

You can select the added organization and click to modify its name.

You can select an organization, and click **X** button to delete it.

Note

- The lower-level organizations will be deleted as well if you delete an organization.
- Make sure there is no person added under the organization, or the organization cannot be deleted.

6.6 Person Management

After adding the organization, you can add person to the organization and manage the added person such as issuing cards in batch, importing and exporting person's information in batch, etc.

Note

Up to 10,000 persons or cards can be added.

6.6.1 Add Person

Person information is necessary for the video intercom system. And when you set linked device for the person, the intercom between intercom devices can be realized.

Steps

1. Select an organization in the organization list and click **Add** on the Person panel to pop up the adding person dialog.

Note

The Person No. will be generated automatically and is editable.

2. Set basic person information.

1) Enter basic information: name, gender, tel, birthday details, effective period and email address.

Note

The length of person name should be less than 15 characters.

2) Click **Add** face to upload the photo.

Note

The picture should be in *.jpg format.

Click Upload	Select the person picture from the local PC to upload it to the client.
Click Take Phone	Take the person's photo with the PC camera.
Click Remote Collection	Take the person's photo with the collection device.

3. Issue the card for the person.

1) Click **Credential → Card** .
2) Click **+** to pop up the Add Card dialog.
3) Select **Normal Card** as **Card Type**.
4) Enter the **Card No.**
5) Click **Read** and the card(s) will be issued to the person.

4. Link the device to the person.

1) Set the linked devices.

Linked Device

You can bind the indoor station to the person.

Note

If you select **Analog Indoor Station** in the Linked Device, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

Room No.

You can enter the room No. of the person.

2) Click **OK** to save the settings.

5. Click **Add** to save the settings.

6.6.2 Modify and Delete Person

Select the person and click **Edit** to open the editing person dialog.

To delete the person, select a person and click **Delete** to delete it.

Note

If a card is issued to the current person, the linkage will be invalid after the person is deleted.

6.6.3 Import and Export Person Information

The person information can be imported and exported in batch.

Steps

1. Exporting Person: You can export the added persons' information in Excel format to the local PC.
   1) After adding the person, you can click **Export Person** to pop up the following dialog.
   2) Click **...** to select the path of saving the exported Excel file.
   3) Check the checkboxes to select the person information to export.
   4) Click **OK** to start exporting.
2. Importing Person: You can import the Excel file with persons information in batch from the local PC.
   1) Click **Import Person**.
   2) You can click **Download Template for Importing Person** to download the template first.
   3) Input the person information to the downloaded template.
   4) Click **...** to select the Excel file with person information.
   5) Click **OK** to start importing.

6.6.4 Get Person Information from Device

If the added device has been configured with person information (including person details, fingerprint, issued card information), you can get the person information from the device and import to the client for further operation.

Steps

Note

This function is only supported by the device the connection mothod of which is TCP/IP when adding the device.

1. In the organization list on the left, click to select an organization to import the persons.
2. Click **Get from Device** to pop up the dialog box.
3. The added device will be displayed.
4. Click to select the device and then click **Get** to start getting the person information from the device.

   Note

   - The person information, including person details, person's fingerprint information (if configured), and the linked card (if configured), will be imported to the selected organization.
   - If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
   - The gender of the persons will be **Male** by default.

6.6.5 Change Person to Other Organization

You can move the person to another organization if needed.

Steps

1. Select the person in the list and click **Change Organization**.
2. Select the organization to move the person to.
3. Click **OK** to save the settings.

6.6.6 Add Person in Batch

Enter a short description of your task here (optional).

Before You Start
Enter the prerequisites here (optional).

Enter the context of your task here (optional).

Steps

1. Enter your first step here.
   Enter the result of your step here (optional).

Example
Enter an example that illustrates the current task (optional).

What to do next
Enter the tasks the user should do after finishing this task (optional).

6.6.7 Issue Card in Batch

You can issue multiple cards for the person with no card issued in batch.

Steps

1. Click **Batch Issue Cards** to enter the dialog page. All the added person with no card issued will display in the Person(s) with No Card Issued list.

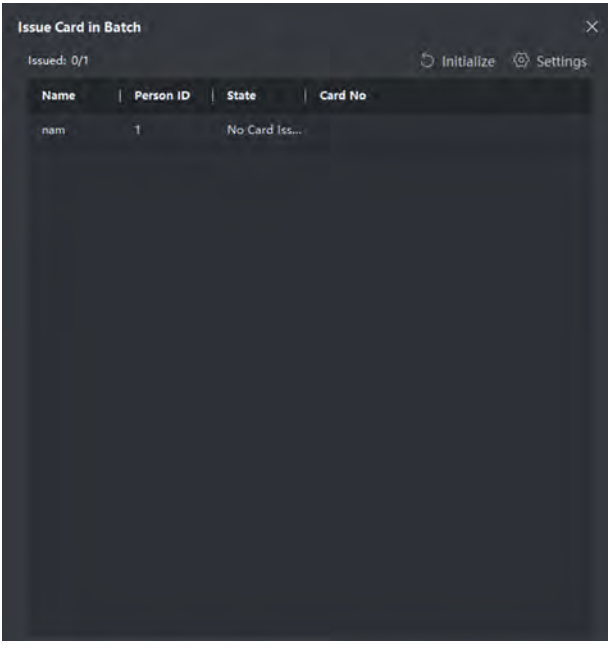


Figure 6-18 Issue Card in Batch

2. Click **Settings**.

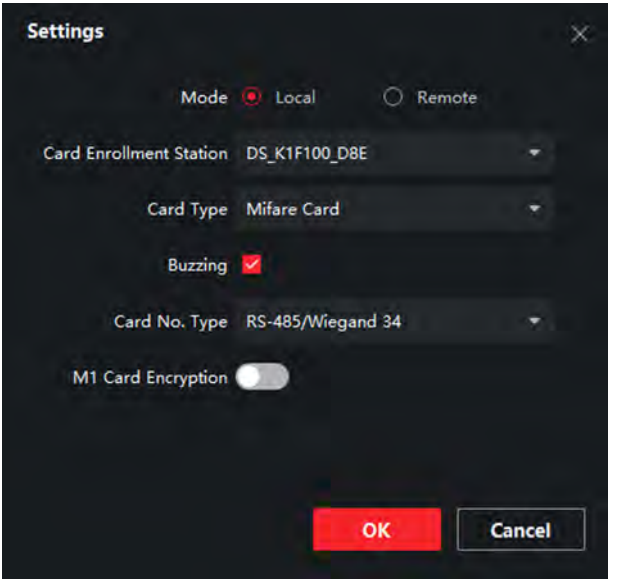


Figure 6-19 Card Settings

3. Select **Card Type** and **Card No. Type**.
4. Click **OK** to save the settings.

Result

After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.

6.6.8 Permission Settings

Add Permissions

Steps

1. On the main page, click **AccessControlInfo → Access Group** to enter the page.
2. Click **+Add** to pop up the adding dialog box.
3. Configure the parameters.

1) Enter the **Name** of the permission.
2) Select the **Template** of the schedule.
3) Check the person to **Selected** according to your needs.
4) Check the device to **Selected** according to your needs.

4. Click **Save**.
5. Check the permission and click **Apply All to Device**.

   The status of the permission displays as **Applied**.
6. **Optional:** Click **Applying Status** to check the details.

Modify/Delete Permissions

On the page of the permission settings, click to edit the parameters of the permission.

Select one or more permissions, click **Delete** to remove the permissions.

6.7 Video Intercom Settings

The Video Intercom Management module provides the function of video intercom, checking call logs and managing notice via the iVMS-4200 Client Software.

Note

For the user with access control module permissions, the user can enter the Access Control module and manage video intercom and search information.

You should add the device to the software and configure the person to link the device in Access Control module before your configuration remotely.

On the main page, click **AccessControlInfo → Video Intercom → Video Intercom** on the left bar to enter the Video Intercom page.

6.7.1 Receive Call from Door Station

Steps

1. Select the client software in the device page to start calling the **iVMS-4200 Client Software** and an incoming call dialog will pop up in the client software.
2. Click **Answer** to answer the call. Or click **Hang Up** to decline the call.
3. After you answer the call, you will enter the In Call window.

- Click to adjust the volume of the loudspeaker.
- Click to adjust the volume of the microphone.
- Click **Hang Up** to hang up the dialog.
- Click to open the door remotely.

Note

- One video intercom device can only connect with one client software.
- The maximum ring duration can be set from 15s to 60s via the Remote Configuration of the video intercom device.
- The maximum speaking duration between indoor station and iVMS-4200 can be set from 120s to 600s via the Remote Configuration of indoor station.
- The maximum speaking duration between door station and iVMS-4200 can be set from 90s to 120s via the Remote Configuration of door station.

6.7.2 Live View via Door Station

Steps

1. On the main page of the client software, click **Main View** to enter the Live View page.
2. In the left list of the window, double-click the device IP or click the play icon to live view.
3. **Optional:** On the Live View page, control-click and select **Capture** to get the picture of the live view.

6.7.3 Release Notice

You can create different types of notices and send them to the residents. Four notice types are available, including Advertising, Property, Alarm and Notice Information.

Before You Start
Make sure the person has been added to the client.

Steps

1. On the video intercom settings page, click **Notice** to enter the page.
2. Click **+Add** to pop up the adding dialog box.
3. Select the person according to your needs.

4. Edit the **Subject**, **Type** and **Information**.
5. Click **View** to select the picture.
6. Click **Send**.

Note

- Up to 63 characters are allowed in the Subject field.
- Up to 6 pictures in the JPGE format can be added to one notice. And the maximum size of one picture is 512KB.
- Up to 1023 characters are allowed in the Information field.

6.7.4 Search Video Intercom Information

Search Call Logs

Steps

1. On the Video Intercom page, click **Call Log** to enter the page.

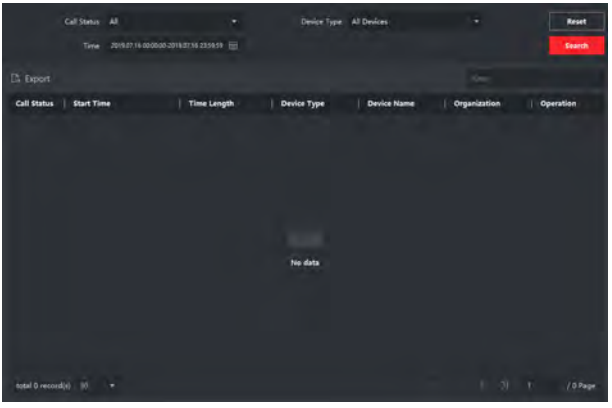


Figure 6-20 Search Call Logs

2. Set the search conditions, including call status, device type, start time and end time.

Call Status

Click ˅ to unfold the drop-down list and select the call status as **Dialed**, **Received** or **Missed**. Or select **All** to search logs with all statuses.

Device Type

Click ˅ to unfold the drop-down list and select the device type as **Indoor Station**, **Door Station**, **Outer Door Station** or **Analog Indoor Station**. Or select **All Devices** to search logs with all device types.

Start Time/End Time

Click the time icon to specify the start time and end time of a time period to search the logs.

Reset the Settings Click **Reset** to reset all the configured search conditions.

3. Click **Search** and all the matched call logs will display on this page.
4. **Optional:** Check the detailed information of searched call logs, such as call status, ring/speaking duration, device name, resident organization, etc.
5. **Optional:** Input keywords in the Search field to filter the desired log.
6. **Optional:** Click **Export** to export the call logs to your PC.

Search Notice

Steps

1. On the Video Intercom page, click **Notice** to enter the page.
2. Set the search conditions, including notice type, start time and end time.
   Type

   Select **Advertising Information**, **Property Information**, **Alarm Information** or **Notice Information** as **Type** according to your needs.

   Start Time/End Time

   Click the time icon to specify the start time and end time of a time period to search the logs.

   Reset the Settings Click **Reset** to reset all the configured search conditiions.
3. Click **Search** and the matched notice will display on this page.
4. **Optional:** Click **Export** to export the notices to your PC.

A. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.

Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.

Figure A-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.

Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.

Figure A-2 Device Command


See Far, Go Further